Attorney Docket No. CISCP733

APPLICATION FOR UNITED STATES PATENT

METHOD AND SYSTEM FOR PROVIDING AUTHORIZATION, AUTHENTICATION, AND ACCOUNTING FOR A VIRTUAL PRIVATE NETWORK

By Inventors:

Wei Luo
170 W. Tasman Drive
San Jose,CA 95134
Citizenship: People's Republic of China

Eric Rosen
250 Apollo Drive
Chelmsford, MA 01824
Citizenship: United States

Assignee: Cisco Technology, Inc.
170 W. Tasman Drive
San Jose, CA 95134

Entity: Large

RITTER, LANG & KAPLAN LLP
12930 Saratoga Ave., Suite D1
Saratoga, CA 95070
(408) 446-8690

METHOD AND SYSTEM FOR PROVIDING AUTHORIZATION, AUTHENTICATION, AND ACCOUNTING FOR A VIRTUAL PRIVATE NETWORK

BACKGROUND OF THE INVENTION

The present invention relates generally to communication networks, and more specifically, to authorization, authentication, and accounting for virtual private networks.

The Internet has changed the way that companies do business. An outgrowth of Internet technology, Virtual Private Networks (VPNs) are transforming the daily method of doing business. Virtual Private Networks serve as private network overlays on public IP network infrastructures such as the Internet. A Virtual Private Network typically uses the Internet as the transport backbone to establish secure links with business partners, extend communications to regional and isolated offices, and significantly decrease the cost of communications for an increasingly mobile workforce. Access VPNs enable users to access corporate resources whenever, wherever, and however they require. Access VPNs encompass analog, dial, ISDN, digital subscriber line (DSL), mobile IP, and cable technologies to securely connect mobile users, telecommuters, or branch offices. There are various types of VPNs: MPLS (Multiprotocol Label Switching, see, RFC 2547 "BGP/MPLS VPNs", E. Rosen et al., March 1999), IPSec (Internet Protocol Security), dial (L2TP, L2F, or PPTP), GRE tunnels, and ATM or Frame Relay PVCs.

A service that Service Providers (SPs) often offer to their VPN customers is managing the remote users access to the customers' VPNs. By managing the remote access, the SP relieves the customer from the responsibility of owning and managing network access servers (NAS) or home gateways for terminating a PPP session. In addition, the SP can benefit from the economies of scale by terminating the remote users of different customers on a shared device and mapping each to the corresponding customer's VPN. The shared device may be a network access server (NAS) or a home gateway, and may be referred to as a virtual home gateway (VHG).

The VHG is a SP device capable of terminating a PPP (Point-to-Point Protocol) sessions of different remote user and mapping each session to the corresponding customer's VPN. (For additional information on PPP see, RFC 1661, "The Point-to-Point Protocol (PPP)", W. Simpson, July 1994)). Traditionally with PPP, the entity that terminates a PPP session is responsible for managing and coordinating all authorization, authentication, and accounting (AAA) operations related to that session.

An AAA server is a software application that performs authorization, authentication, and accounting functions, usually by interacting with network access servers, or gateways and databases or directories containing user information. AAA servers provide a security mechanism to protect a company's investments by permitting only certain entities (such as individuals or system processes) to access those investments, by governing what those entities can do once they are authenticated, and by logging or auditing the actions that are preformed for future reference and troubleshooting purposes. The SP's AAA server may be, for example, a RADIUS (Remote Authentication Dial In User Service) server or a TACACS (Terminal Access Controller Access Control System Plus) server. Fig. 1 illustrates a prior art system for providing authorization, authentication, and accounting operations at a service provider. The remote user 10 communicates with the SP VHG 12 via dial-up, DSL, or other type of connection. The SP has an AAA server 14 that includes a database 16 containing information on all remote users that have access to a VPN. After authenticating and authorizing the remote user 10, the SP connects the remote user with the VPN through its enterprise server (or firewall) 18. The VPN has its own private AAA server 20. As further described below, the SP's AAA server 14 may communicate directly with the VPN's private AAA server 20. The following describes details of the authorization, authentication, and accounting operations of this conventional system and drawbacks associated with this system.

Authorization is the process of giving permission to an entity to access a system resource. For example, network access can be restricted based on the identity of a client. Authorization provides the function of associating a remote user with a customer VPN and possibly applying policies specific to that particular VPN which may not be specific to the remote user. Authorization is usually based on either the user's domain name (e.g., @cisco.com) or, in the case of dial-up, the DNIS (Dial Number Information Service). The SP has two main options for performing the authorization functions. One is to configure the authorization information locally on the VHG. This is appropriate for SPs who do not have an AAA server. The second option is for the VHG to send an AAA request to the SP's AAA server to authorize the remote user.

Authentication is the process of verifying the identity of an entity. This process is usually done by exchanging information to prove one's identity. This information may take the form of a password, token, or one-time password, for example. In order for the SP to perform customer complete authentication of the customers' remote users, it must maintain a complete and up-to-date database of all the remote users of each customer. This has a clear drawback for large customers. One solution to this problem is to do proxy authentication. Proxy authentication requires the SP to have an AAA server. At session initiation time, the VHG is only capable of sending one AAA request per remote user. The same request must be used to both authorize and authenticate the remote user's PPP session.

The VHG first sends an AAA request to the SP AAA server for the incoming remote user. The SP's AAA server authorizes the remote user and associates it with a specific customer's VPN. The SP AAA server also determines the address of the VPN customer's AAA server. The SP AAA server proxies the AAA request to the customer's AAA server. The customer AAA server authenticates the remote user and responds to the SP AAA server with either success or failure. The SP AAA then sends a response back to the VHG with the results of the authorization and authentication operations. Drawbacks to this approach are that it requires the SP to have an AAA server and requires the SP AAA server and the customer AAA server to communicate. This can pose a security risk. Since the customer AAA server is in the customer VPN and the SP AAA server is either in the SP's management VPN or in its global routing table, routes must be redistributed (exported, imported, and filtered) between the customer VPN's routing table and the SP VPN's routing table so that the two AAA servers can communicate. It is possible to accomplish this route redistribution in a secure fashion, but it is a rather complex operation that is prone to configuration errors.

Accounting enables a network manager to keep track of the services and resources that are used by the users. The accounting process collects information such as the connection time, identity, and billing information. Conventional VHGs can only send accounting records to a single group of AAA servers that must be reachable via a global routing table. As a result, the VHG only sends accounting records to the SP's AAA server. However, because the VPN customers are also interested in receiving accounting records for their remote users, the SP's AAA server can be configured to save a copy of the accounting records and then proxy the same record to the VPN customer's AAA server. The process of proxying accounting records suffers from the same drawbacks discussed above for proxy authentication.

If the PPP session terminates on an access server or a home gateway inside the customer network, then the customer is typically responsible for the AAA operations. However, if the PPP session terminates on an SP's VHG, then the SP is responsible for the AAA operations. As described above, there are many drawbacks to the SP performing AAA operations and what is needed is a more secure and easier to configure mechanism for performing AAA operations in an SP managed remote access environment.

SUMMARY OF THE INVENTION

A method and system for providing authentication in a virtual private network is disclosed. The virtual private network includes a private AAA server. The method generally includes receiving a request from a remote user for connection with a virtual private network at a virtual home gateway and associating the remote user with the virtual private network The virtual home gateway sends a request to authenticate the remote user to the AAA server. The remote user is then connected to the virtual private network if the AAA server authenticates the user.

The authorization of the remote user may be performed by an AAA server connected to the virtual home gateway if the service provider has an AAA server. The accounting may be performed at the AAA servers of both the service provider and the virtual private network, only one of the AAA servers, or different accounting information may be sent to each AAA server. The virtual home gateway may include a plurality of routing tables for different virtual private networks. The virtual home gateway has access to a database comprising information such as virtual private network IDs and addresses of the virtual private network AAA servers. The AAA server of the virtual private network is

coupled to a database comprising information on remote users that are allowed to access to the virtual private network.

A system of the present invention generally includes a virtual home gateway configured to receive requests from a remote user for connection with a virtual private network, send a request to authenticate the remote user to the AAA server of the virtual private network, and connect the remote user to the virtual private network. The system further includes a database for storing addresses of virtual private network AAA servers and a processor operable to look up the address of the virtual private network AAA server based on information received from the remote user.

In another aspect of the invention, a computer program product for providing authentication in a virtual private network generally includes code that receives a request from a remote user for connection with a virtual private network at a virtual home gateway and that associates the remote user with the virtual private network. The product further includes code that sends a request to authenticate the remote user from the virtual home gateway to the AAA server and code that connects the remote user to the virtual private network if the AAA server authenticates the user. A computer-readable storage medium is provided for storing the codes.

The above is a brief description of some deficiencies in the prior art and advantages of the present invention. Other features, advantages, and embodiments of the invention will be apparent to those skilled in the art from the following description, drawings, and claims.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a diagram illustrating a prior art network for providing AAA operations by a service provider to a remote user.

Fig. 2 is a diagram illustrating a network utilizing a system of the present invention for providing AAA operations for a VPN.

Fig. 3 is a diagram illustrating additional detail of a network utilizing the system of Fig. 2.

Fig. 4 is a system block diagram of a computer system that can be utilized to execute software of an embodiment of the present invention.

Fig. 5 is a flowchart illustrating a process of the present invention for providing authorization and authentication in a virtual private network.

Fig. 6 is a flowchart illustrating an accounting process for the virtual private network.

Corresponding reference characters indicate corresponding parts throughout the several views of the drawings.

DETAILED DESCRIPTION OF THE INVENTION

The following description is presented to enable one of ordinary skill in the art to make and use the invention. Descriptions of specific embodiments and applications are provided only as examples and various modifications will be readily apparent to those skilled in the art. The general principles described herein may be applied to other embodiments and applications without departing from the scope of the invention. Thus, the present invention is not to be limited to the embodiments shown, but is to be accorded the widest scope consistent with the principles and features described herein. For purpose of clarity, details relating to technical material that is known in the technical fields related to the invention have not been described in detail.

Referring now to the drawings, and first to Fig. 2, a system of the present invention is shown. The system eliminates the need for an AAA proxy and all the associated security hazards by allowing an AAA server located within a virtual private network to communicate directly with a service provider. As further described below, the system allows service providers to eliminate their AAA servers. Furthermore, the service provider's virtual home gateway may be configured to communicate with a plurality of different virtual private network AAA servers. Authorization is preferably performed at the service provider while the authentication is performed at the virtual private network, thus providing a clear separation between authorization and authentication functions.

The present invention operates in the context of a data communication network including multiple network elements. The network includes a service provider that manages remote access of different customers to their enterprise server. The service provider network includes a virtual home gateway (VHG) 30 that is accessed by remote user 10. The VHG 30 may be a network access server (NAS) or a home gateway, for example. VHG 30 is preferably a shared device having a plurality of routing tables (A, B, C, D) for different virtual private networks. The service provider may include an AAA server 32, however, it is not necessary. The AAA server 32 includes a database 34 containing addresses of VPNs' AAA servers and may include other information such as VPN IDs. Each VPN has an associated group of remote users that are not individually identified, but identified by indicators such as domain name (e.g., cisco.com), DNIS (phone number or ID stream for a dial network (e.g., 1-800-xxx-xxxx)), circuit ID for a DSL network, or wireless network ID, for example. The virtual private network includes an enterprise server (firewall) 36, AAA server 38, and database 40. The database includes a list of all remote users that are allowed access to the VPN. For example, the database 40 may include a list of usernames (e.g., Joe@cisco.com). Thus, the SP AAA server 32 is used to authorize an entire VPN, while the VPN AAA server 38 authenticates and authorizes individual VPN users. Accounting requests are preferably sent to both AAA servers 32, 38 since it is easy to match start and stop records based on the full username, and in the case of dispute both the service provider and the VPN customer have the same level of accounting details.

Fig. 3 illustrates additional detail of the system of Fig. 2. The remote user may include, for example, dial-up client 50 (with access to the SP through a PSTN 52), PPP over ATM (PPPoA) 54 or PPP over Ethernet (PPPoE) 56 having access through a DSL access network 58, or Layer 2 Tunneling Protocol (L2TP), having access through the Internet 62, or any other remote access systems and methods, as is well known by those skilled in the art. The service provider VHG 30 operates as a Provider Edge (PE) router and receives data from the remote user. The service provider also includes PE router 68 which transmits data to a Customer Edge (CE) router 70 at the customer VPN. It is to be understood that the network shown and described herein is only one example of a network that may utilize the system and method of the present invention and that the system and method may be used in different types of networks without departing from the scope of the invention.

Fig. 4 shows a system block diagram of computer system 78 that may be used to execute software of an embodiment of the invention. The computer system 78 includes memory 82 which can be utilized to store and retrieve software programs incorporating computer code that implements aspects of the invention, data for use with the invention, and the like. Exemplary computer readable storage media include CD-ROM, floppy disk, tape, flash memory, system memory, and hard drive. Additionally, a data signal embodied in a carrier wave (e.g., in a network including the Internet) may be the computer readable storage medium. Computer system 78 further includes subsystems such as a central processor 80, fixed storage 84 (e.g., hard drive), removable storage 86 (e.g., CD-ROM drive), and one or more network interfaces 94. Other computer systems suitable for use with the invention may include additional or fewer subsystems. For example, computer system 78 may include more than one processor 80 (i.e., a multi-processor system) or a cache memory. The computer system 78 may also include a display, keyboard, and mouse (not shown) for use as a host.

The system bus architecture of computer system 78 is represented by arrows 96 in Fig. 4. However, these arrows are only illustrative of one possible interconnection scheme serving to link the subsystems. For example, a local bus may be utilized to connect the central processor 80 to the system memory 82. Computer system 78 shown in Fig. 4 is only one example of a computer system suitable for use with the invention. Other computer architectures having different configurations of subsystems may also be utilized. Communication between computers within the network is made possible with the use of communication protocols, which govern how computers exchange information over a network.

Figs. 5 and 6 are flowcharts illustrating authorization, authentication, and accounting operations performed with the above-described system. A user first contacts the VHG 30 at step 100 (Fig. 5). When VHG 30 receives an incoming PPP session, it passes the authorization entity, such as domain name or DNIS, to the SP AAA server 32. When the VHG 30 sends an AAA request, it is routed using either the SP's management VPN or a global routing table. If an SP AAA server is used, the VHG sends two AAA requests. The first request is for authorizing the remote user and is routed to the SP's AAA server using either SP's management VPN or the SP's global routing table. The second request is for authenticating the remote user and is routed to the customer's AAA server using the VPN customer's routing table. The VHG 30 may authorize the remote user 10 either locally or by sending a request to the SP AAA server 38. If the user is not authorized by the VHG 30, the session is terminated (steps 102 and 103). A successful authorization operation associates the remote user with a VPN. The SP AAA server 32 returns the VPN AAA server address along with a VPN ID and other information necessary to communicate with the customer's AAA server. The information may include, for example, a key for use with a Radius server. The VHG 30 determines which VPN the customer belongs to based on the VPN ID. The profile is retrieved from the SP AAA server 32 (step 104) and applied to the VPN customer at the SP (step 106). The VPN ID binds the profile to routing table in VHG 30 (step 108). The VPN AAA server address is interpreted by the VHG 30 within the correct VPN context. The VHG 30 looks up the VPN ID to find the corresponding virtual routing forwarding (VRF) instance. In order to communicate with the VPN AAA server 38, the VHG 30 has a local address belonging to the VRF. The address is used as source address to send user requests to the VPN AAA server 38. The VHG 30 sends an AAA request to the customer's AAA server 38 to authenticate the remote user 10 (step 110). Upon successful authentication, the VPN AAA server 38 responds to VHG 30 with a success message, which may contain per-user authorization data. The VHG 30 applies the per-user configuration to the PPP session. The VHG 30 then continues setting up the remote user's PPP session and when initialization is complete, packets will start to flow to and from the remote user 10 (steps 112 and 114). If the authentication is not successful the connection is terminated (steps 112 and 113).

For accounting, the VHG 30 preferably sends any accounting request related to a given remote user to the AAA servers of both the SP and the customer. Once the SP receives authentication from the VPN AAA server 38 (step 140), the SP sends start records to the SP AAA server 32 and VPN AAA server 38 (steps 142, 144). The accounting record sent to the SP's AAA server 32 is routed using either the SP's management VPN or the SP's global routing table.

The accounting record sent to the customer's AAA server 38 is routed using the customer VPN's routing table. If the customer is not interested in accounting records then the accounting records can be sent only to the SP AAA server 32. If the SP does not have an AAA server, the accounting records are sent to the VPN AAA server 38 only. Also, different accounting information may be sent to the SP AAA server 32 and the VPN AAA server 38. For example, the customer may be interested only in the duration of a connection and the number of packets or bytes which are transferred in both directions. The SP may be interested in additional information related to the utilization of the resources on the VHG 30. At step 146 the connection is closed and a stop is sent to the SP AAA server 32 and the VPN AAA server 38 (steps 148 and 150).

As can be observed from the foregoing, the present invention has numerous advantages. The system and method of the present invention allow service providers to operate without dedicated AAA servers and provides a clear separation between the authorization and authentication functions. Furthermore, the system allows different accounting information to be sent to the SP and the customer.

Although the present invention has been described in accordance with the embodiments shown, one of ordinary skill in the art will readily recognize that there could be variations made to the embodiments without departing from the scope of the present invention. Accordingly, it is intended that all matter contained in the above description and shown in the accompanying drawings shall be interpreted as illustrative and not in a limiting sense.